

UNITED STATES DISTRICT COURT
DISTRICT OF RHODE ISLAND

IN THE MATTER OF A SEARCH OF:

79 HIGH STREET, ASHAWAY, RHODE
ISLAND;

THE PERSON OF VICTOR TAN CHEN; and

A 2021 NISSAN ALTIMA BEARING
RHODE ISLAND REGISTRATION 1UA466,
VIN: 1N4BL4DV6MN361342

Case No.25-SW-015-PAS

25-SW-016-PAS

25-SW-018-PAS

Filed Under Seal

Affidavit in Support of Applications for Search Warrant

I, ATF Special Agent Michael J. Carpentier, being duly sworn, state:

1. I am a Special Agent employed by the Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”). As such, I am a law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18 of the United States Code; that is, an officer empowered by law to conduct investigations of, and make arrests for, offenses enumerated in Section 2516 of Title 18. I have been employed by ATF as a Special Agent since August of 2022. Previously, I served as a full-time, certified, Police Officer in the state of New Hampshire for approximately eight years. During my tenure as a Police Officer, I also served in the role of Detective with the Hooksett (NH) Police Department. I graduated from Walden University with a Bachelor’s degree in Nutritional Science and from Southern New Hampshire University with a Master’s degree in Business Administration. I attended and successfully completed training at the New Hampshire Police Academy, which is conducted at the New Hampshire Police Standards and Training Council in Concord, New Hampshire. I attended and successfully completed the Department of Homeland Security Criminal Investigator Training Program and the ATF Special Agent Basic

Training program, both of which are conducted at the Federal Law Enforcement Training Center in Glynn County, Georgia.

2. I have received specialized training in firearms identification and the investigation of firearm-related offenses, both as a Police Officer and Special Agent. I have participated in investigations involving persons who are in possession of firearms in furtherance of the distribution of narcotics, and the use of firearms in the commission of violent acts. I have participated in hundreds of investigations involving individuals who are distributing illegal narcotics. In such investigations, I have coordinated the controlled purchases of illegal narcotics, utilizing confidential sources. I have had the opportunity to interview subjects who have been arrested for distribution of and conspiracy to distribute controlled substances. I have conducted electronic and physical surveillance of individuals involved in illegal narcotics distribution and the unlawful possession of firearms. I have received training both formal and on-the-job, in the provisions of the federal firearms and narcotics laws administered under Titles 18, 21 and 26 of the United States Code. I know that motor vehicles are often used to transport illegal firearms and controlled substances. I have been the affiant on applications to search and seize evidence from persons, buildings, vehicles, and for the installation of tracking devices on motor vehicles. Through my training and experience in conducting narcotics investigations, I know that drug and firearms traffickers who use motor vehicles are often difficult to surveil as they engage in erratic driving and countersurveillance techniques to avoid being followed by law enforcement. I know that tracking the movements of drug and firearms traffickers in motor vehicles often leads to the location of the target's source of supply and stash houses and enables law enforcement to follow a suspect and identify co-conspirators in drug and

firearms trafficking. Furthermore, based upon your affiants training and experience, I know that cellular telephones, drugs, and firearms are often kept in the vehicle of the trafficker/possessor.

3. Through my training and experience, I have become familiar with the habits, methods, routines, practices, and procedures commonly employed by persons engaged in criminal activity and other organized criminal activity. I am familiar with the “street” language used by firearm and/or drug traffickers via electronic communication facilities, as well as the methods they use to disguise conversation and operations. I know drug traffickers commonly communicate over cellular telephone and through messaging applications which are encrypted, like WhatsApp, and Telegram, to avoid detection. I am also aware that drug traffickers often use multiple cellular telephones, some use separate phones for customers and some for suppliers. I know that unlawful traffickers of controlled substances frequently place orders with their sources of supply via cellular phone either by text messages or telephone calls, and cellular devices retain evidence of such communications long after the conversation or communication has occurred. In my experience, I find that text messages confirming drug transactions, amounts owed, customer lists and ledgers can be found on the cellular telephones. Also, I am aware that GPS history and calendars on phones can assist law enforcement in determining stash locations and meet locations for drug transactions.

4. Based upon training and experience, and conversations with senior agents, unlawful traffickers of controlled substances keep their drug, proceeds, ledgers, drug packaging material and other associated drug paraphernalia in their residences. I know that drug traffickers also keep banking records and use banks to deposit proceeds and often retain these records in their homes, vehicles and on their persons.

5. Furthermore, based upon your affiants training and experience, I know that cellular telephones, drugs, and firearms are often kept in the vehicle or the trafficker/possessor.
6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other Agents, Task Force Officers, and Providence Police Department personnel. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

Purpose of Affidavit

7. Based on the facts presented in this Affidavit, there is probable cause to believe that violations of 21 U.S.C. §§ 841 (distribution and possession with intent to distribute controlled substances) and 846 (conspiracy to possess with intent to distribute controlled substances) (the “SUBJECT OFFENSES”) have been committed, are being committed, and will be committed by Victor TAN CHEN.
8. Additionally, because probable cause exists to believe TAN CHEN committed the “SUBJECT OFFENSES”, for the reasons set forth below, probable cause also exists to believe that evidence, fruits, and instrumentalities of the “SUBJECT OFFENSES” will be found in the following places:
 - a. the residence of 79 High Street, Ashaway, Rhode Island, which is further described as a single-family brown colored two-story residence, including a basement. The residence features blue shutters, a white front door and a car port, with a horseshoe style driveway. 79 High Street, Ashaway, Rhode Island is located at the corner of Ashaway Clarks Falls Road and Robin Road (“SUBJECT PREMISES”), further described in Attachment A-1 for the items described in Attachment B-1.
 - b. the person of Victor TAN CHEN, Y.O.B. 1993 (“SUBJECT PERSON”) , further described in Attachment A-2 for the items described in Attachment B-2; and
 - c. a 2021 blue Nissan Altima bearing Rhode Island Registration 1UA466, VIN:

1N4BL4DV6MN361342, (“SUBJECT VEHICLE”), further described in Attachment A-3 for the items described in Attachment B-3.

9. Further, probable cause exists to believe that items described in Attachment B-1, Attachment B-2, and Attachment B-3, will be found in the locations set forth above (items in Attachment B-1 will be found in the SUBJECT PREMISES, items in Attachment B-2 will be found on the SUBJECT PERSON, and items in Attachment B-3 will be found in the SUBJECT VEHICLE).

Facts Establishing Probable Cause

10. The United States, including the ATF and the Providence Police Department Organized Crime Intelligence Bureau, is conducting a criminal investigation of Victor TAN CHEN and co-conspirators regarding the violations of 21 U.S.C. §§ 841 (distribution and possession with intent to distribute controlled substances) and 846 (conspiracy to possess with intent to distribute controlled substances).
11. In the month of September 2024, your affiant was in contact with a Confidential Informant (hereinafter referred to as “CI”)¹ who had knowledge of Victor TAN CHEN selling firearms and distributing narcotics. The CI stated that he knows TAN CHEN and is familiar with his appearance.² The CI stated that TAN CHEN communicates with the CI through his Telegram profile “Chinaville” and via text messaging. Telegram is a messaging application that allows users to send messages, create channels for broadcasting, communicate through end-to-end encrypted voice and video calls, share videos, pictures and make money transfers and online payments. Telegram allows users to register with the application with a telephone

¹ Throughout this affidavit, the CI will be referred to as “he” regardless of his or her gender. The CI is known to be credible, while previously providing information that has led to the arrest, conviction of individuals engaged in illegal activity and the recovery of evidence.

² I know that TAN CHEN has convictions in RI State court from 2021 for manufacture/delivery of a controlled substance and possession of a firearm by a prohibited person (two counts). Defendant was sentenced to time to serve in State Corrections.

number or anonymously without a telephone number. The CI provided a telephone number over which the CI communicated with for TAN CHEN, (929) 630-3288 (the 3288 number).

12. Your affiant conducted law enforcement database queries of the 3288 number which revealed the service provider for the 3288 number as AT&T, with the likely subscriber of the account to be Victor TAN CHEN. During the investigation, law enforcement tentatively identified the girlfriend of TAN CHEN to be Morgan BOSS (Y.O.B 1996). Your affiant conducted a law enforcement database query of BOSS, which revealed an associated address of 79 High Street, Ashaway, Rhode Island. Your affiant conducted the same law enforcement database query for TAN CHEN, which revealed an associated address of 79 High Street, Ashaway, Rhode Island, the SUBJECT PREMISES.

13. For the following reasons there is probable cause to believe that TAN CHEN resides at the SUBJECT PREMISES

- a) Law enforcement identified the girlfriend of TAN CHEN to be Morgan Boss. While utilizing law enforcement databases, law enforcement identified an associated address of Morgan Boss to be 79 High Street, Ashaway, Rhode Island. Law enforcement later conducted surveillance of 79 High Street, Ashaway, Rhode Island. Law enforcement observed the SUBJECT VEHICLE parked in the driveway of 79 High Street, Ashaway, Rhode Island. Law enforcement conducted a registration query of the SUBJECT VEHICLE and determined the SUBJECT VEHICLE was registered to TAN CHEN however, at an address different than .
- b) During this ongoing investigation, your affiant observed a white 2014 Ford Escape, bearing Connecticut Registration BE58912, parked in the driveway at 79 High Street, Ashaway, Rhode Island. Your affiant conducted a registration query on Connecticut Registration BE58912, which yielded information that the vehicle is registered to Morgan Boss. Through a previously installed internet protocol camera (described

below), your affiant has consistently observed the white Ford Escape parked at 79 High Street, Ashaway, Rhode Island.

c) In the weeks leading up to the controlled purchases in January 2025, described below, your affiant reviewed surveillance footage from a previously installed internet protocol (IP) camera. This camera allows law enforcement to monitor the SUBJECT PREMISES from its position in the area.³ Your affiant observed the SUBJECT VEHICLE parked in the driveway of 79 High Street, Ashaway, Rhode Island during all hours of the day. Your affiant has observed TAN CHEN, freely, coming and going from the SUBJECT PREMISES, at all hours, and in a manner that suggested TAN CHEN has unrestricted access to it. Law enforcement have also conducted mobile surveillance of TAN CHEN, who was seen leaving the SUBJECT PREMISES and presumably arrived at TAN CHEN's place employment.

14. During the month of January 2025, the ATF conducted two controlled purchases of cocaine which were arranged through TAN CHEN. The arrangements to set up the purchases were made by the CI, at the direction of the ATF but not in the presence of law enforcement, the CI and TAN CHEN communicated and arranged the purchase via text at the 3288 number. The CI arranged to meet TAN CHEN at a pre-determined location, in nearby Connecticut to complete the purchase of cocaine, close to the SUBJECT PREMISES . The communications between the CI and TAN CHEN were observed by law enforcement, who verified the 3288 number was the contacted phone number by the CI and that the content appeared consistent with a conversation regarding a narcotics transaction.

³ The images captured from the pole camera are images which would be visible to persons in a public place on the street in the area of SUBJECT PREMISES.

15. Prior to the start of the controlled purchase, your affiant met with the CI at a pre-determined brief location. Your affiant searched the CI and the vehicle the CI would be operating, for contraband and additional monies, which yielded negative results. The CI was provided with a quantity of ATF funds to complete the purchase of cocaine from TAN CHEN. The CI left the pre-determined meet location, while under continuous surveillance by law enforcement. The CI arrived at the pre-determined meet location without stopping.
16. Shortly after the CI arrived at the pre-determined meet location law enforcement observed TAN CHEN via physical surveillance, exiting the SUBJECT PREMISES. TAN CHEN was observed entering the driver seat of the SUBJECT VEHICLE. Law enforcement officers were positioned approximately .5 miles down High Street. Via physical surveillance TAN CHEN was seen driving in the direction of law enforcement and towards the pre-determined meet location. Moments later, law enforcement observed TAN CHEN and began physical surveillance of the SUBJECT VEHICLE, as the SUBJECT VEHICLE proceeded to the pre-determined meet location.⁴
17. Law enforcement observed the SUBJECT VEHICLE arrive at the pre-determined meet location. Law enforcement officers who were familiar with TAN CHEN, the SUBJECT PERSON, were able to positively identify the driver of the SUBJECT VEHICLE as TAN CHEN⁵. Law enforcement observed the CI exit their vehicle and enter the SUBJECT VEHICLE. The CI later exited the SUBJECT VEHICLE and entered their vehicle. The CI returned to a pre-determined debriefing location, while under continuous surveillance by law enforcement. While at the debriefing location, the CI relinquished a quantity of suspected cocaine to your affiant. The CI stated that TAN CHEN arrived at the meeting location, that

⁴ This was not continuous, so as to not be detected by the driver of the SUBJECT VEHICLE, due to the close proximity of the SUBJECT PREMISES to the pre-determined meet location. A matter of minutes had surpassed before law enforcement observed the SUBJECT VEHICLE travelling to the meet location. The timeframe was consistent with uninterrupted travel.

⁵ It should be noted that TAN CHEN has changed the color and style of his hair during the course of this investigation, including blonde- however investigators are familiar with his physical appearance, including height and weight.

the CI entered into TAN CHEN's vehicle and handed over the purchase funds to TAN CHEN.

18. The suspected cocaine was subsequently field tested, which revealed a presumptive positive presence of cocaine. Law enforcement conducted a post-operation search of the CI and the vehicle the CI was operating for contraband and additional monies, which yielded negative results.
19. Your affiant observed through the pole camera, that the SUBJECT VEHICLE arrived back at the SUBJECT PREMISES, after the planned operation.
20. Again during the month of January 2025, the CI contacted TAN CHEN at the 3288 number to purchase cocaine. The CI arranged to meet TAN CHEN at a pre-determined location to complete the purchase of cocaine. The communications between the CI and TAN CHEN were observed by law enforcement, who verified the 3288 number was the number contacted phone number by the CI.
21. Prior to the start of the planned operation, your affiant met the CI at a pre-determined meet location. Your affiant drove the CI to a pre-determined brief location. Your affiant searched the CI and the CI's vehicle for contraband and additional monies which yielded negative results. The CI was provided with a quantity of ATF funds to complete the purchase of cocaine from TAN CHEN.
22. Prior to the CI's arrival at the pre-determined meet location, but after the arrangements were made between CI and TAN CHEN, via physical surveillance, law enforcement observed the SUBJECT VEHICLE arrive at the SUBJECT PREMISES. Law enforcement observed TAN CHEN exit the SUBJECT VEHICLE and enter the SUBJECT PREMISES, accompanied by two other individuals.
23. While under continuous surveillance and without stopping, the CI departed the pre-determined brief location and arrived at the pre-determined meet location. Shortly after the CI's arrival at the pre-determined meet location, law enforcement observed one of the

individuals who had arrived at the SUBJECT PREMISES with TAN CHEN, exit the SUBJECT PREMISES. Law enforcement observed the individual entering the SUBJECT VEHICLE and depart the SUBJECT PREMISES.

24. Minutes later, law enforcement observed the SUBJECT VEHICLE arrive at the pre-determined meet location. While under continuous surveillance, law enforcement observed the CI exiting their vehicle and enter the SUBJECT VEHICLE. Shortly thereafter, the CI exited the SUBJECT VEHICLE and re-entered their vehicle. While under continuous surveillance by law enforcement and without stopping, the CI departed the pre-determined meet location and arrived at the pre-determined debrief location.
25. While at the debrief location, the CI relinquished the purchased, suspected cocaine, to a member of law enforcement. The suspected cocaine was later field tested by law enforcement, which yielded the presumptive positive presence of cocaine. Law enforcement conducted a post operational search of the CI and the vehicle the CI was operating for contraband and additional monies, which yielded negative results. The CI explained that he was at the meet location and observed the SUBJECT VEHICLE arrive. The CI explained that someone other than TAN CHEN was driving the SUBJECT VEHICLE. The CI explained that he handed over the purchase funds, the amount the CI and TAN CHEN had agreed upon as the purchase price, to this individual and this individual handed him the quantity of cocaine agreed upon in his communications with TAN CHEN.
26. After the SUBJECT VEHICLE left the meeting location, law enforcement conducted both physical surveillance and viewed the pole camera footage and observed the SUBJECT VEHICLE return to the SUBJECT PREMISES.⁶

⁶ This was not continuous surveillance so as to not be detected by the driver of the SUBJECT VEHICLE, however, the SUBJECT VEHICLE returned to the SUBJECT PREMISES, in a timeframe consistent with the SUBJECT VEHICLE driving directly to the location.

27. Based on the facts that the controlled purchases were set up by TAN CHEN, that the SUBJECT VEHICLE was driven directly to the meet location and returned immediately to the SUBJECT PREMISES, I believe that the SUBJECT PREMISES is a location in which drugs are stored and the proceeds (money paid by the CI) of drug dealing can be found. Although the second controlled delivery of suspected cocaine was made by a person other than TAN CHEN, I believe that an agreement existed between TAN CHEN and the person delivering to traffic cocaine. The communications between the CI to set up this second delivery was made over TAN CHEN's phone and the person delivering the drugs was with TAN CHEN moments before and used TAN CHEN's vehicle, the SUBJECT VEHICLE.

Digital Devices⁷ and Request for Biometric Unlocking of Those Devices

28. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

- a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with

⁷ As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

more recently downloaded or viewed content and may also be recoverable months or years later.

- b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.
 - c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.
 - d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.
29. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during execution of a search warrant for a number of reasons, including the following:
- a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time,

particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

- b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

30. Based upon my involvement and the involvement of other agents in this investigation, I know that drug traffickers regularly communicate using cellular telephones, which has been confirmed in this case and TAN CHEN's communications with the CI.

31. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant.

I seek this authority based on the following:

- a. I know from my training and experience, as well as information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can

unlock a device once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device though his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law

enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who

is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

32. Based on my training, experience and working knowledge with this case, I know that TAN CHEN did not limit his communications to the phone but that he uses a messaging app. Thus, I believe it is likely that there will be several apps and social media networking platforms and that TAN CHEN used these to communicate to facilitate violations of the SUBJECT OFFENSES.

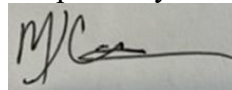
CONCLUSION

33. Based upon the above, I believe that there is probable cause to believe that violations of 21 U.S.C. §§ 841 (distribution and possession with intent to distribute controlled substances) and 846 (conspiracy to possess with intent to distribute controlled substances) (the SUBJECT OFFENSES) have been committed, are being committed, and will be committed by Victor TAN CHEN.

34. Furthermore, probable cause exists to believe that evidence, fruits, and instrumentalities of these SUBJECT OFFENSES will be found in the places set forth in Attachments A-1, A-2 and A-3, and permission is sought to search in those places for the items listed in Attachments B-1, B-2 and B-3.

Sworn to under the pains and penalties of perjury.

Respectfully submitted,



Michael J. Carpentier
Special Agent
Bureau of Alcohol, Tobacco, Firearms and
Explosives

Attested to by the applicant in accordance with the requirements of Fed.
R. Crim. P. 4.1 by _____

(specify reliable electronic means)

Date

Judge's signature

City and State

Printed name and title

Attachment A-1

Premises to be Searched (SUBJECT PREMISES)

The residence located at 79 High Street, Ashaway, RI, described, as a one-story, single-family residence located on the corner of Robin and High Streets in Ashaway, RI. The structure is brown with blue shutters on the window. The front door faces High Street. Viewing the home from High Street, the driveway is to the left of the front door and there is a car-port type structure attached to the residence (left of the front door when viewing from street. The front door is white in color. At the rear of the structure, a bulkhead door is visible. SUBJECT PREMISES is depicted in photos below.



Front of SUBJECT PREMISES, view from High Street.



Side and rear view of SUBJECT PREMISES, view from Robin Street.

AttachmentA-2

Person to be Searched

VICTOR TAN CHEN (SUBJECT PERSON)

VICTOR TAN CHEN is an Asian male, with black or blonde hair and brown eyes, approximately 5'6" and with a slim build, approximately 150 lbs. He appears to be his known age, of approximately 31-32 years old. SUBJECT PERSON is depicted in the photograph below-the color and style of his hair has changed during the course of the investigation, however his facial features and height/weight descriptions remain the same.



Attachment A-3

Vehicle to be Searched (SUBJECT VEHICLE)

Victor Tan Chen's 2021 blue Nissan Altima bearing Rhode Island Registration 1UA466,
VIN: 1N4BL4DV6MN361342.

Attachment B-1

Particular Things to be Seized (SUBJECT PREMISES)

The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 21, United States Code, Sections 841(a) (1) and 846 (drug trafficking and conspiracy) (herein referred to as the SPECIFIED FEDERAL OFFENSES), namely:

- a) Any controlled substance, controlled substance analogue, or listed chemical;
- b) Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing devices, balloons, packaging materials, containers, and money counters;
- c) Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;
- d) United States currency over \$1,000 or bearer instruments worth over \$1,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first \$1,000), and data, records, documents, or information (including electronic mail, messages over applications and social media, and photographs) pertaining to, obtaining, possessing, using, applications for, or transferring money over \$1,000, such as bank account records, cryptocurrency records and accounts;
- e) FINANCIAL RECORDS: All financial records of or relating to VICTOR TAN CHEN and his nominees, assignees, or co-conspirators, including but not limited to financial statements, balance sheets, income statements, cash flow statements, ledgers, journals, accounts receivable, accounts payable leases, bank statements, deposit tickets, deposit items, checks, checkbooks, check registers, passbooks, money orders, cashier's checks, official checks, bank

drafts, wire transfer instructions and receipts, withdrawal slips, credit memos, debit memos, signature cards, account applications, automatic teller machine receipts, safe deposit box applications, safe deposit box keys, credit card statements, charge slips, receipts brokerage statements, buy and sell orders and other items evidencing the obtaining, secreting, transfer, or concealment of assets and the obtaining, secreting, transfer, concealment, or expenditure of money;

f) Items showing unexplained wealth or evidencing the proceeds derived from illicit drug trafficking, including but not limited to large sums of money, expensive vehicles, financial instruments, precious metals, jewelry, and real estate, and documents evidencing the procuring or leasing of these items;

g) Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances, or drug customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;

h) TRAVEL DOCUMENTS: All documents evidencing or relating to foreign or domestic travel of VICTOR TAN CHEN; or his co-conspirators, including but not limited to airline tickets, tickets for other means of transport, credit card receipts, travel vouchers, hotel receipts, restaurant receipts, gas receipts, notes, schedules, other receipts evidencing travel, boarding passes, itineraries, luggage tags and receipts, frequent flyer statements and awards, car rental receipts and statements, photographs of travel locations, maps, written directions to a location, visas, passports, United States and foreign customs declaration receipts and forms;

- i) Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to- talk functions, as well as all received or missed incoming calls;
- j) STORAGE UNIT RECORDS: All records reflecting the ownership or control of storage units including keys, contracts, leases, payments, and inventories;
- k) Shipping records, to include any and all receipts (USPS, FedEx, UPS, and DHL) for parcels shipped to VICTOR TAN CHEN
- l) Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;
- m) Records, documents, programs, applications or materials, or evidence of the absence of same, including text, instant, and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;
- n) Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;
- o) Contents of any calendar or date book;
- p) Global Positioning System (“GPS”) coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and
- q) Any digital device (SEE BELOW- INCLUDING CELLULAR TELEPHONES AND TABLETS) which itself or which contains evidence, contraband, fruits, or instrumentalities of the SPECIFIED FEDERAL OFFENSES, and forensic copies thereof.
- r) Firearms.

s) Keys to a 2021 blue Nissan Altima bearing Rhode Island Registration

1UA466, VIN: 1N4BL4DV6MN361342 and to the SUBJECT PREMISES.

With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized;

1. evidence of who used, owned, or controlled the digital device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
2. evidence of software that would allow others to control the cellular phone, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. evidence of the lack of such malicious software;
4. evidence indicating how and when the digital device was accessed or used to determine the chronological context of device's access, use, and events relating to the crimes under investigation and to the phone user;
5. evidence indicating the device's user's knowledge and/or intent as it relates to the crimes under investigation;
6. evidence of the attachment to the device of other storage devices or similar containers for electronic evidence;
7. evidence of programs (and associated data) that are designed to eliminate data from the device;
8. evidence of the times the device was used;
9. passwords, encryption keys, and other access devices that may be necessary to access the cellular phone;
10. records of or information about Internet Protocol addresses used by the device and
11. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
12. With respect to any and all electronically stored information in digital devices and cellular devices, in addition to the information described herein, agents may also access, record and seize the following:
 - i. Telephone numbers of incoming/outgoing calls stored in the call registry;
 - ii. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;
 - iii. Any incoming/outgoing text messages relating to the above criminal violations;
 - iv. Telephone subscriber information;
 - v. The telephone numbers stored in the cellular telephone and/or PDA;

- vi. Records relating to the use, possession, and control of any cellular telephones and cellular devices seized;
- vii. Any other electronic information stored in the memory and/or accessed by the active electronic features of the digital or cellular phone/device including but not limited to photographs, videos, e-mail, and voice mail relating to the above SPECIFIED FEDERAL OFFENSES.

As used herein, the terms “records,” “documents,” “programs,” “applications,” and “materials” include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

As used herein, the term “digital device” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, memory cards, and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

In searching digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

- a. Law enforcement personnel or other individuals assisting law enforcement personnel (the “search team”) will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.
- b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, “hidden,” or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools such as “EnCase” and “FTK” (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access

data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

Attachment B-2

Particular Things to be Seized (SUBJECT PERSON VICTOR TAN CHEN)

- a. Any CELLULAR DEVICE/ TELEPHONE which itself or which contains evidence, contraband, fruits, or instrumentalities of violations of Title 21, United States Code, Sections 841(a) (1) and 846 (drug trafficking and conspiracy) (referred to as the SPECIFIED FEDERAL OFFENSES), and forensic copies thereof.
- b. Any controlled substances or controlled substance analogue;

With respect to any cellular device/telephone containing evidence falling within the scope of the foregoing categories of items to be seized;

1. evidence of who used, owned, or controlled the cellular device/telephone at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
2. evidence of software that would allow others to control the cellular device/telephone, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. evidence of the lack of such malicious software;
4. evidence indicating how and when the cellular device/ telephone accessed or used to determine the chronological context of device's access, use, and events relating to the crimes under investigation and to the phone user;
5. evidence indicating the cellular device's/telephone user's knowledge and/or intent as it relates to the crimes under investigation;
6. evidence of the attachment to the cellular device/telephone of other storage devices or similar containers for electronic evidence;
7. evidence of programs (and associated data) that are designed to eliminate data from the device;
8. evidence of the times the cellular device/telephone was used;
9. passwords, encryption keys, and other access devices that may be necessary to access the cellular device/telephone;
10. records of or information about Internet Protocol addresses used by the cellular device/telephone and
11. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

12. With respect to any and all electronically stored information in the cellular device/s/telephone, in addition to the information described herein, agents may also access, record and seize the following:
 - i. Telephone numbers of incoming/outgoing calls stored in the call registry;
 - ii. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;
 - iii. Any incoming/outgoing text messages relating to the above criminal violations;
 - iv. Telephone subscriber information;
 - v. The telephone numbers stored in the cellular telephone and/or PDA;
 - vi. Records relating to the use, possession, and control of any cellular devices/telephones seized;
 - vii. Any other electronic information stored in the memory and/or accessed by the active electronic features of the cellular phone/device including but not limited to photographs, videos, e-mail, and voice mail relating to the above SPECIFIED FEDERAL OFFENSES.

As used herein, the terms “records,” “documents,” “programs,” “applications,” and “materials” include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on the cellular device/telephone and any forensic copies thereof.

II. SEARCH PROCEDURE FOR CELLULAR DEVICE/TELEPHONE

In searching cellular devices/telephones (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

- c. Law enforcement personnel or other individuals assisting law enforcement personnel (the “search team”) will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.
- d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.
 - i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to

determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, “hidden,” or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

iv. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

v. The search team may use forensic examination and searching tools such as “EnCase” and “FTK” (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a cellular device/telephone, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

c. If the search determines that a cellular device/telephone does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

d. If the search determines that a cellular device/telephon does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

e. If the search determines that a cellular device/telephone is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the cellular device/telephone, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

f. The government may also retain a cellular device/telephone if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the cellular device/telephone or files contained therein is/are encrypted.

g. After the completion of the search of the cellular devices/telephones, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

Attachment B-3

Particular Things to be Seized (SUBJECT VEHICLE)

The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 21, United States Code, Sections 841(a) (1) and 846 (drug trafficking and conspiracy) (herein referred to as the SPECIFIED FEDERAL OFFENSES), namely:

- Any controlled substance, controlled substance analogue, or listed chemical;
- Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing devices, balloons, packaging materials, containers, and money counters;
- Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;
- United States currency over \$1,000 or bearer instruments worth over \$1,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first \$1,000), and data, records, documents, or information (including electronic mail, messages over applications and social media, and photographs) pertaining to, obtaining, possessing, using, applications for, or transferring money over \$1,000, such as bank account records, cryptocurrency records and accounts;
- FINANCIAL RECORDS: All financial records of or relating to VICTOR TAN CHEN and his nominees, assignees, or co-conspirators, including but not limited to financial statements, balance sheets, income statements, cash flow statements, ledgers, journals, accounts receivable, accounts payable leases, bank statements, deposit tickets, deposit items, checks, checkbooks, check registers, passbooks, money orders, cashier's checks, official checks, bank

drafts, wire transfer instructions and receipts, withdrawal slips, credit memos, debit memos, signature cards, account applications, automatic teller machine receipts, safe deposit box applications, safe deposit box keys, credit card statements, charge slips, receipts brokerage statements, buy and sell orders and other items evidencing the obtaining, secreting, transfer, or concealment of assets and the obtaining, secreting, transfer, concealment, or expenditure of money;

- Items showing unexplained wealth or evidencing the proceeds derived from illicit drug trafficking, including but not limited to large sums of money, expensive vehicles, financial instruments, precious metals, jewelry, and real estate, and documents evidencing the procuring or leasing of these items;

- Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances, or drug customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;

- TRAVEL DOCUMENTS: All documents evidencing or relating to foreign or domestic travel of TAN CHEN; or his co-conspirators, including but not limited to airline tickets, tickets for other means of transport, credit card receipts, travel vouchers, hotel receipts, restaurant receipts, gas receipts, notes, schedules, other receipts evidencing travel, boarding passes, itineraries, luggage tags and receipts, frequent flyer statements and awards, car rental receipts and statements, photographs of travel locations, maps, written directions to a location, visas, passports, United States and foreign customs declaration receipts and forms;

- Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to- talk functions, as well as all received or missed incoming calls;
- STORAGE UNIT RECORDS: All records reflecting the ownership or control of storage units including keys, contracts, leases, payments, and inventories;
- Shipping records, to include any and all receipts (USPS, FedEx, UPS, and DHL) for parcels shipped to TAN CHEN
- Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;
- Records, documents, programs, applications or materials, or evidence of the absence of same, including text, instant, and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;
- Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;
- Contents of any calendar or date book;
- Global Positioning System (“GPS”) coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and
- Any digital device (SEE BELOW- INCLUDING CELLULAR TELEPHONES AND TABLETS) which itself or which contains evidence, contraband, fruits, or instrumentalities of the SPECIFIED FEDERAL OFFENSES, and forensic copies thereof.
- Firearms.
- Keys to the SUBJECT VEHICLE.

With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized;

1. evidence of who used, owned, or controlled the digital device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
2. evidence of software that would allow others to control the cellular phone, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. evidence of the lack of such malicious software;
4. evidence indicating how and when the digital device was accessed or used to determine the chronological context of device's access, use, and events relating to the crimes under investigation and to the phone user;
5. evidence indicating the device's user's knowledge and/or intent as it relates to the crimes under investigation;
6. evidence of the attachment to the device of other storage devices or similar containers for electronic evidence;
7. evidence of programs (and associated data) that are designed to eliminate data from the device;
8. evidence of the times the device was used;
9. passwords, encryption keys, and other access devices that may be necessary to access the cellular phone;
10. records of or information about Internet Protocol addresses used by the device and
11. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
12. With respect to any and all electronically stored information in digital devices and cellular devices, in addition to the information described herein, agents may also access, record and seize the following:
 - i. Telephone numbers of incoming/outgoing calls stored in the call registry;
 - ii. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;
 - iii. Any incoming/outgoing text messages relating to the above criminal violations;
 - iv. Telephone subscriber information;
 - v. The telephone numbers stored in the cellular telephone and/or PDA;
 - vi. Records relating to the use, possession, and control of any cellular telephones and cellular devices seized;
 - vii. Any other electronic information stored in the memory and/or accessed by the active electronic features of the digital or cellular phone/device including but

not limited to photographs, videos, e-mail, and voice mail relating to the above SPECIFIED FEDERAL OFFENSES.

As used herein, the terms “records,” “documents,” “programs,” “applications,” and “materials” include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

As used herein, the term “digital device” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, memory cards, and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

In searching digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

e. Law enforcement personnel or other individuals assisting law enforcement personnel (the “search team”) will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.

f. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to

determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, “hidden,” or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

vi. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

vii. The search team may use forensic examination and searching tools such as “EnCase” and “FTK” (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

h. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

i. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

j. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

k. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

l. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.